REMARKS

1. Applicant thanks the Examiner for the Examiner's comments, which have greatly assisted Applicant in responding.

Claim Objections

2. Claims 25 and 33 are objected to by the Examiner because the word "interactively" in the preamble is not spelled correctly and the Examiner requested appropriate correction.

Applicant respectfully thanks the Examiner and points out to the Examiner that correct word is "iteratively." Support can be found in the Specification on page 24, line 8 through page 25, line 13. Text from page 25, lines 10-13 appear as follows (emphasis added):

> 6) **Repeating steps 2 through 5 until a comprehensive desired policy is defined.** At this point the end user may start monitoring network traffic on a continuous basis, and using generated reports as input for further policy refinement.

Accordingly, Claims 25 and 33 have been amended. Applicant is of the opinion that the objections are overcome. Therefore, Applicant respectfully requests that the Examiner withdraw the objections.

35 U.S.C. §103

3. Claims 1-40 are rejected by the Examiner under 35 U.S.C. §103(a) as being unpatentable over Vaid *et al* U.S. Patent No. 6,502,131 (hereinafter Vaid) in view of Rogers *et al* U.S. Patent No. 5,557,747 (hereinafter Rogers).

Applicant respectfully disagrees.

(a) Claim 1 (and 13)

Claim 1 appears as follows (emphasis added):

1. (original) A system for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action, comprising:

a policy specification file;

a network monitor processor for processing network packet data collected from said subject network; and

a policy monitoring component for receiving and processing said policy specification file, and receiving and **processing said processed network packet data to assign dispositions to network events** contained in said network packet data.

The Examiner stated that Vaid discloses "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data" and cited Vaid's Figure 8 and Reference Nos. 808-811.

Vaid's Figure 8 and text related to Reference Nos. 801-807, as well as 808-811, appear as follows (emphasis added):

> The present method occurs at start, which is step 801, for example. In general, a flow of information or data **or packets** of information enter a gateway point, where the present tool sits. **The present method classifies (step 803) the flow of information**. Groups of flows can be referred to as traffic classes, but are not limited to such classes. Classes also can be defined by source, destination, application, file types, URLs, and other features. Other examples of classes were previously noted, but are not limited to these classes. In general, step 803 classifies the flow of information received into one of a plurality of predetermined classes.
>
> **The present tool measures parameters for each of the classes in step 805**, which were received, for example. These parameters are based upon the policy or rule, which may be applied in a later step. As merely an example, parameters include the class itself, file sizes, and other information, which can be used by the policy or rule to apply the policy or rule to improve the quality of service for the network. After measuring the parameters, the present method applies a time stamp (step 807) on the parameters to correlate the class of information received to a time, for example.

A step of determining whether to apply a policy occurs in the next step 809. For example, **if the class and the time (and the link state in some embodiments) meet predetermined settings, the policy is applied to the class in step 811 through branch 810.** Alternatively, if one of the elements including the class, the time, or the link state do not meet the predetermined settings, the policy does not apply **and the process continues to measure parameters through branch 808.** Alternatively, the process continues to measure parameters through branch 813 after the policy is applied to the flow of information for the class.

Depending upon the application, the policy is used to improve the quality of service of the network by performing at least one of a number of functions for the class of information from the flow. These **functions include, among others, bandwidth guarantees, bandwidth limits, setting priorities, admission control.** The present process can also halt or stop as shown in step 815. The steps occur, in part, by way of the modules, which were previously described, but can also occur using other techniques including a combination of hardware and software, for example. These sequence of steps are merely illustrative and should not limit the scope of the claims herein. One of ordinary skill in the art would recognize other modifications, alternatives, and variations.

Nowhere does Vail in the above or elsewhere teach or disclose "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data." Applicant respectfully requests that the Examiner show where Vaid discloses assigning dispositions to network events.

Nowhere does Rogers teach or disclose "'a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data."

Accordingly, in view of the above, neither prior art of reference alone or in combination teach, disclose, suggest, or motivate all claim limitations of Claims 1 and 13. Therefore, Claims 1 and 13 and the respective dependent claims, are in

condition for allowance. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

(b) Claim 33 (and 25)

Amended Claim 33 appears as follows (emphasis added):

> 33. (currently amended) A system for ~~interatively~~ iteractively developing network security policy for a network, said system comprising:
> means for creating an initial network security policy file;
> means for ensuring said initial network security policy file is uploaded to a machine on said network;
> means for running a network monitor on said machine to collect said network traffic;
> means for said network monitor outputting said collected network traffic in an output file, and passing said output file to a policy monitor;
> means for said policy monitor analyzing said collected network traffic;
> means for storing said analyzed network traffic in a database;
> means for examining said analyzed network traffic in said database by querying said database using a query tool; ~~and~~
> means for modifying said initial network security policy file as needed; and
> means for repeating from said means for ensuring network security policy file is uploaded through said means for modifying said network security policy file until a comprehensive and desired policy file is attained.

The Examiner stated that Vaid further includes a system for ... developing network security policy for a network, the system comprising: means for modifying the initial network security policy file as needed until a comprehensive and desired policy file is attained. The Examiner then cited Vaid, Figs. 15 and 19.

Related text for Fig. 15 appear as follows (emphasis added):

> (Col. 22, lines 9-11)
> FIG. 15 is a simplified graphical user interface 1500 **for adding or specifying an additional chart** according to the present invention.

Vaid further clarifies chart as follows (emphasis added):

(Col. 21, lines 48-54)
Furthermore, the present tool **has other types of charts such as a bar chart, a pie chart, and the like**. Of course, the parameter being profiled and monitored depends upon the application.

In an alternative embodiment, **the present invention provides a user interface for modifying the plots or charts**, such as the one previously described, as well as others. FIG. 14 is a simplified interface tool 1400 used to modify chart styles, scales, charting intervals etc.

(Col. 21, lines 62-67)
Numerous chart options 1407 exist. For example, options include, among others, **a legend, a value bar, a vertical grid, a horizontal grid, and vertical labels**. To select any one of these options, the user clicks onto the box located next to the option or enters the underlined key designating the option. Chart options also include a gallery 1409, either

Applicant points out that nowhere in the above does Vaid teach or disclose "means for modifying the initial network security policy file as needed until a comprehensive and desired policy file is attained" because Vaid is teaching adding or specifying a chart. A chart is simply a display of data: data of the display are not added or modified.

Related text for Fig. 19 appear as follows (emphasis added):

(Col. 27, lines 23-38)
As merely an example, FIG. 19 illustrates a screen 1900 or graphical user interface (GUI) from the manager, which serves to illustrate the look and feel of a policy management interface. The present Fig. is merely an illustration and should not limit the scope of the claims herein. The user interface has been configured as rows and columns, where the rows represent a traffic class or category. Each column represents one of many features for each class or category of traffic. The feature can be, for example, a rule 1901, a sender 1903, a receiver 1905, a service 1907, time 1909, bandwidth allocated 1911, priority 1913, and admissions 1915. Through this GUI, the present invention uses policies to define both monitoring and control actions. These rules incorporate: a traffic class which defines a flow or set of flows including

source, destination, application and file type. Traffic classes can incorporate users and groups

In view of the above, Applicant asserts that neither Vaid nor Rogers teach, disclose, suggest, or motivate "means for repeating from said means for ensuring network security policy file is uploaded through said means for modifying said network security policy file until a comprehensive and desired policy file is attained."

Accordingly, in view of the above, neither prior art of reference alone or in combination teach, disclose, suggest, or motivate all claim limitations of Claims 33 and 25. Therefore, Claims 33 and 25 and the respective dependent claims, are in condition for allowance. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

4. It should be appreciated that Applicant has elected to amend the Claims solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making such amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

CONCLUSION

Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent. The Examiner is invited to call to discuss the response.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862